FIG. 1
PRIOR ART

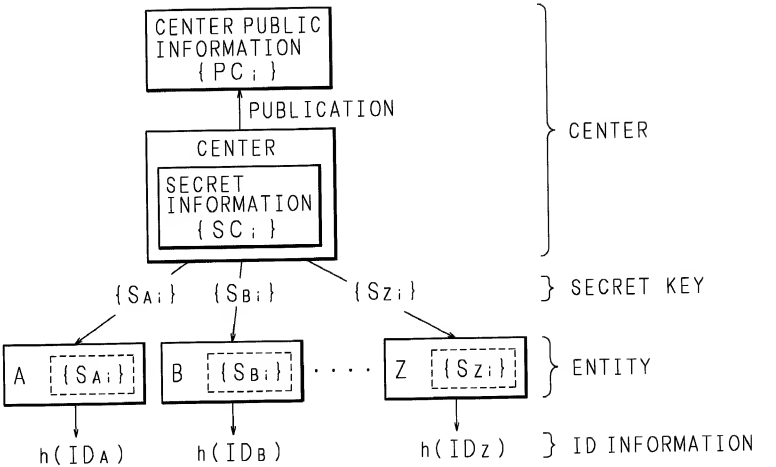


FIG. 2

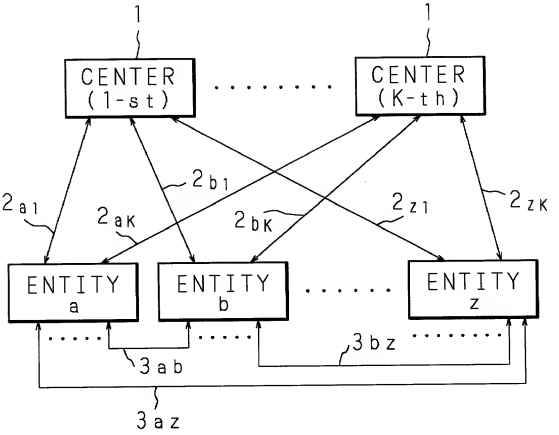

1
1
CENTER
(1-st)
CENTER
(K-th)
2a1
2aK
2b1
2bK
2z1
2zK
ENTITY
a
ENTITY
b
ENTITY
z
3ab
3bz
3az

FIG. 3

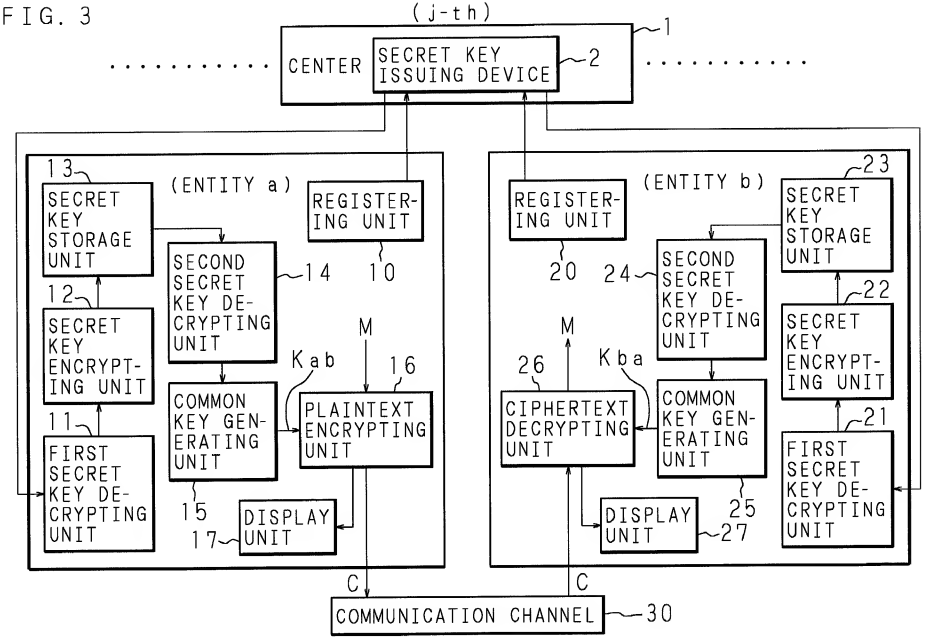

(j-th)
CENTER
SECRET KEY ISSUING DEVICE
1
2
(ENTITY a)
13
SECRET KEY STORAGE UNIT
12
SECRET KEY ENCRYPTING UNIT
11
FIRST SECRET KEY DECRYPTING UNIT
SECOND SECRET KEY DECRYPTING UNIT
14
REGISTERING UNIT
10
COMMON KEY GENERATING UNIT
15
Kab
M
16
PLAINTEXT ENCRYPTING UNIT
DISPLAY UNIT
17
(ENTITY b)
REGISTERING UNIT
20
23
SECRET KEY STORAGE UNIT
22
SECRET KEY ENCRYPTING UNIT
21
FIRST SECRET KEY DECRYPTING UNIT
24
SECOND SECRET KEY DECRYPTING UNIT
M
26
Kba
CIPHERTEXT DECRYPTING UNIT
COMMON KEY GENERATING UNIT
25
DISPLAY UNIT
27
C
C
COMMUNICATION CHANNEL
30

FIG. 4

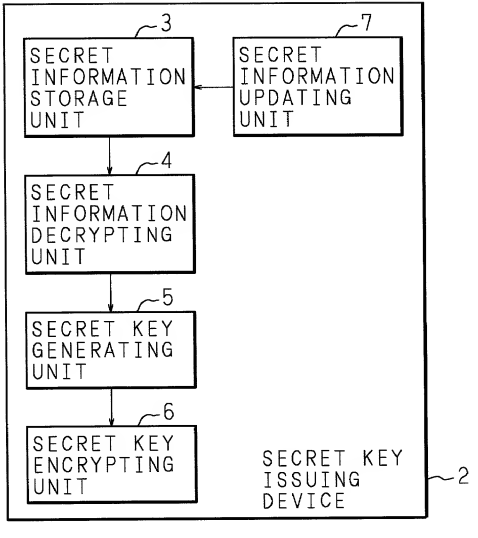

3
SECRET INFORMATION STORAGE UNIT
7
SECRET INFORMATION UPDATING UNIT
4
SECRET INFORMATION DECRYPTING UNIT
5
SECRET KEY GENERATING UNIT
6
SECRET KEY ENCRYPTING UNIT
SECRET KEY ISSUING DEVICE
2

FIG. 5

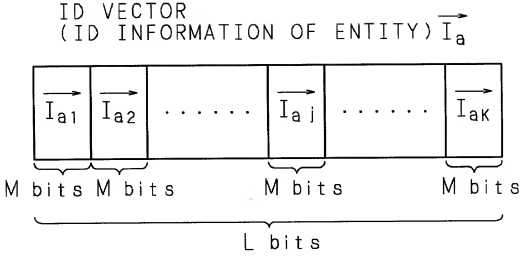

ID VECTOR
(ID INFORMATION OF ENTITY) $\overrightarrow{I_a}$
$\overrightarrow{I_{a1}}$
$\overrightarrow{I_{a2}}$
.....
$\overrightarrow{I_{aj}}$
.....
$\overrightarrow{I_{aK}}$
M bits
M bits
M bits
M bits
L bits

FIG. 6

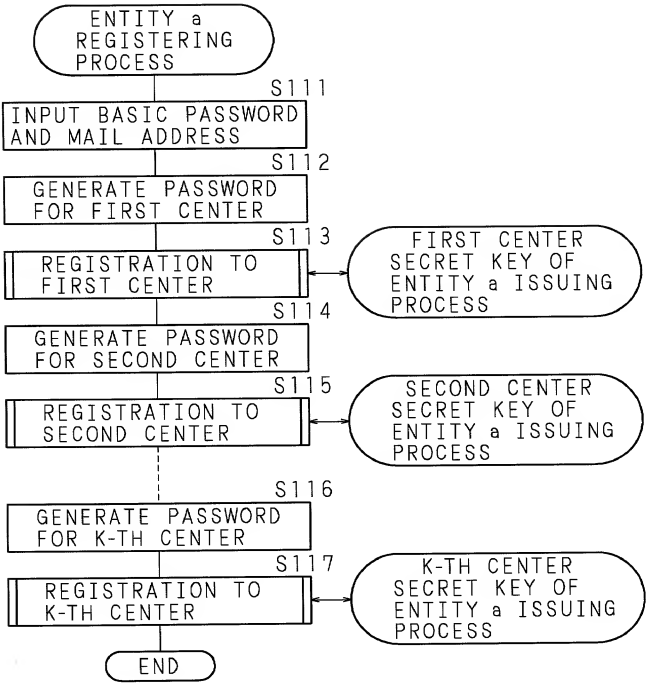

ENTITY a REGISTERING PROCESS
S111
INPUT BASIC PASSWORD AND MAIL ADDRESS
S112
GENERATE PASSWORD FOR FIRST CENTER
S113
REGISTRATION TO FIRST CENTER
FIRST CENTER SECRET KEY OF ENTITY a ISSUING PROCESS
S114
GENERATE PASSWORD FOR SECOND CENTER
S115
REGISTRATION TO SECOND CENTER
SECOND CENTER SECRET KEY OF ENTITY a ISSUING PROCESS
S116
GENERATE PASSWORD FOR K-TH CENTER
S117
REGISTRATION TO K-TH CENTER
K-TH CENTER SECRET KEY OF ENTITY a ISSUING PROCESS
END

FIG. 7

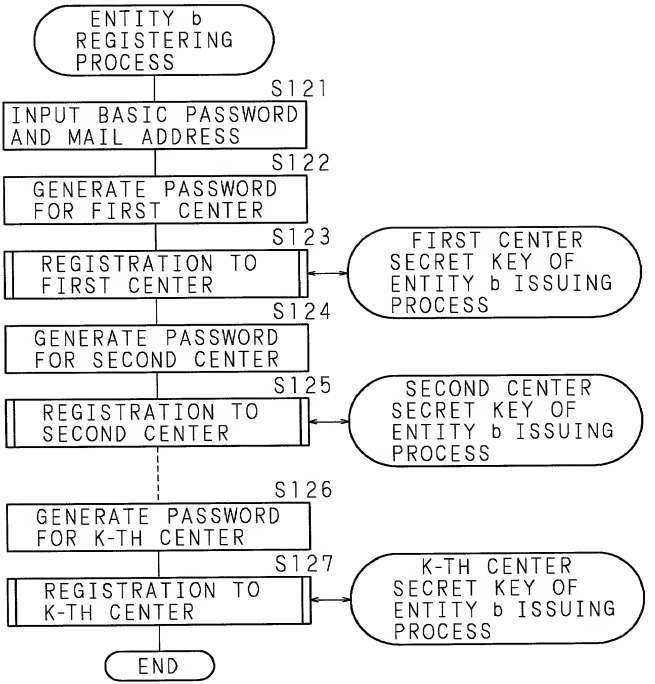

ENTITY b REGISTERING PROCESS
S121
INPUT BASIC PASSWORD AND MAIL ADDRESS
S122
GENERATE PASSWORD FOR FIRST CENTER
S123
REGISTRATION TO FIRST CENTER
FIRST CENTER SECRET KEY OF ENTITY b ISSUING PROCESS
S124
GENERATE PASSWORD FOR SECOND CENTER
S125
REGISTRATION TO SECOND CENTER
SECOND CENTER SECRET KEY OF ENTITY b ISSUING PROCESS
S126
GENERATE PASSWORD FOR K-TH CENTER
S127
REGISTRATION TO K-TH CENTER
K-TH CENTER SECRET KEY OF ENTITY b ISSUING PROCESS
END

FIG. 8A

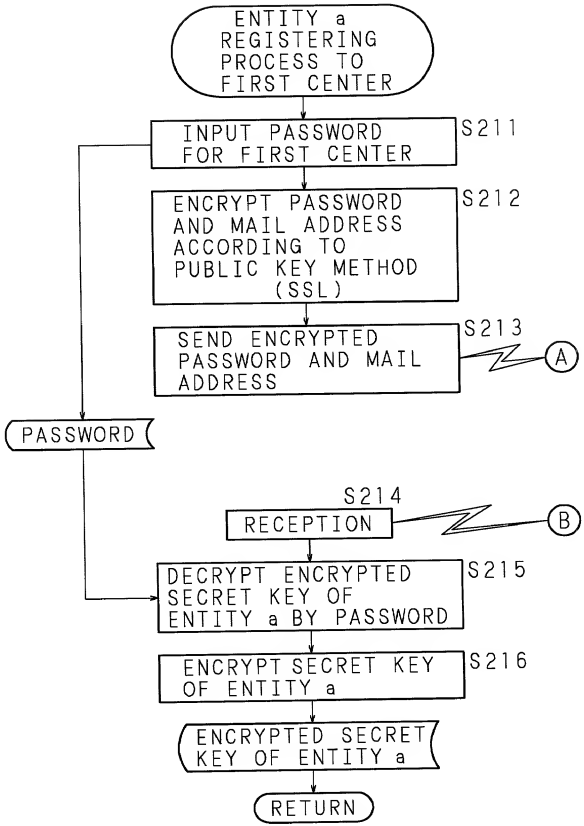

ENTITY a REGISTERING PROCESS TO FIRST CENTER
INPUT PASSWORD FOR FIRST CENTER
S211
ENCRYPT PASSWORD AND MAIL ADDRESS ACCORDING TO PUBLIC KEY METHOD (SSL)
S212
SEND ENCRYPTED PASSWORD AND MAIL ADDRESS
S213
A
PASSWORD
S214
RECEPTION
B
DECRYPT ENCRYPTED SECRET KEY OF ENTITY a BY PASSWORD
S215
ENCRYPT SECRET KEY OF ENTITY a
S216
ENCRYPTED SECRET KEY OF ENTITY a
RETURN

FIG. 8B

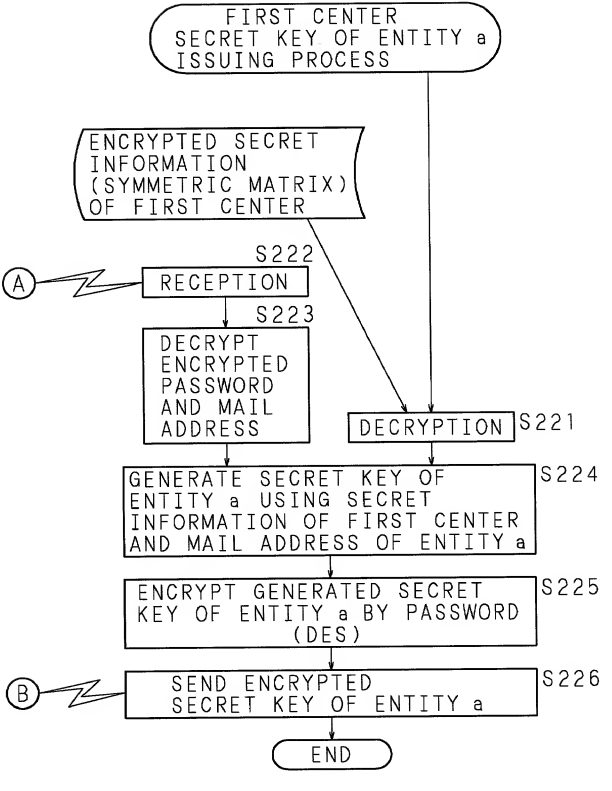

FIRST CENTER SECRET KEY OF ENTITY a ISSUING PROCESS
ENCRYPTED SECRET INFORMATION (SYMMETRIC MATRIX) OF FIRST CENTER
S222
A
RECEPTION
S223
DECRYPT ENCRYPTED PASSWORD AND MAIL ADDRESS
DECRYPTION
S221
GENERATE SECRET KEY OF ENTITY a USING SECRET INFORMATION OF FIRST CENTER AND MAIL ADDRESS OF ENTITY a
S224
ENCRYPT GENERATED SECRET KEY OF ENTITY a BY PASSWORD (DES)
S225
B
SEND ENCRYPTED SECRET KEY OF ENTITY a
S226
END

FIG. 9A

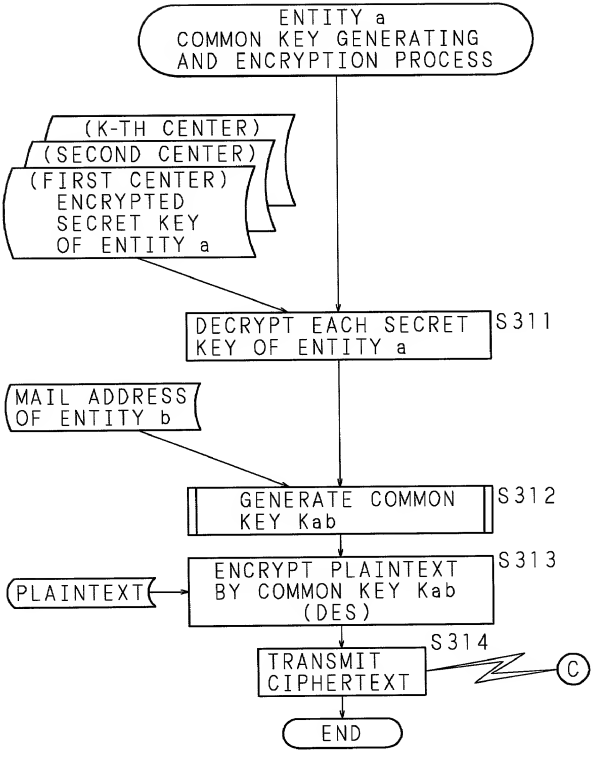

ENTITY a
COMMON KEY GENERATING
AND ENCRYPTION PROCESS
(K-TH CENTER)
(SECOND CENTER)
(FIRST CENTER)
ENCRYPTED
SECRET KEY
OF ENTITY a
DECRYPT EACH SECRET
KEY OF ENTITY a
S311
MAIL ADDRESS
OF ENTITY b
GENERATE COMMON
KEY Kab
S312
ENCRYPT PLAINTEXT
BY COMMON KEY Kab
(DES)
S313
PLAINTEXT
TRANSMIT
CIPHERTEXT
S314
C
END

FIG. 9B

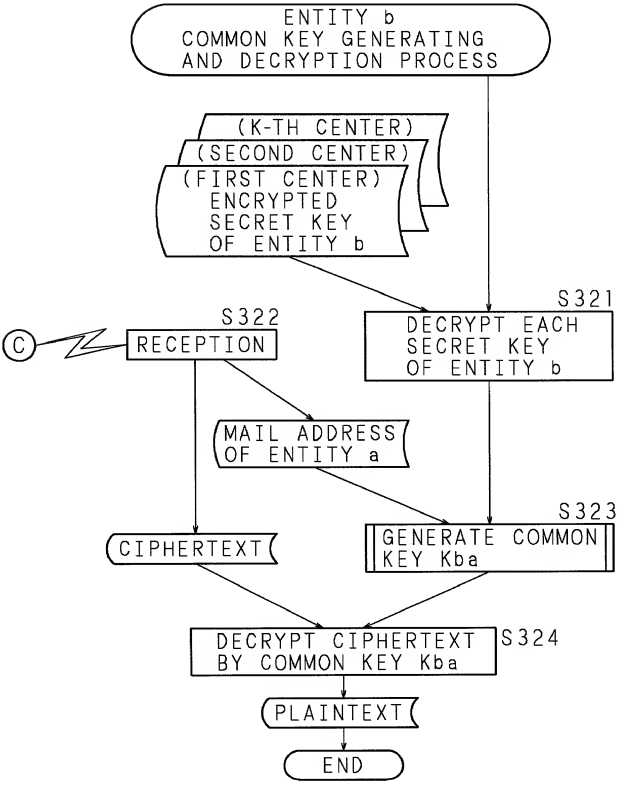

ENTITY b
COMMON KEY GENERATING
AND DECRYPTION PROCESS
(K-TH CENTER)
(SECOND CENTER)
(FIRST CENTER)
ENCRYPTED
SECRET KEY
OF ENTITY b
S321
DECRYPT EACH
SECRET KEY
OF ENTITY b
S322
C
RECEPTION
MAIL ADDRESS
OF ENTITY a
S323
CIPHERTEXT
GENERATE COMMON
KEY Kba
DECRYPT CIPHERTEXT
BY COMMON KEY Kba
S324
PLAINTEXT
END

FIG. 10

EXAMPLE OF MAIL ADDRESS

(a) ATTACHMENT OF DOMAIN NAME thomas@xyz.co.jp
DOMAIN NAME

(b) NO ATTACHMENT OF DOMAIN NAME thomas

FIG. 11

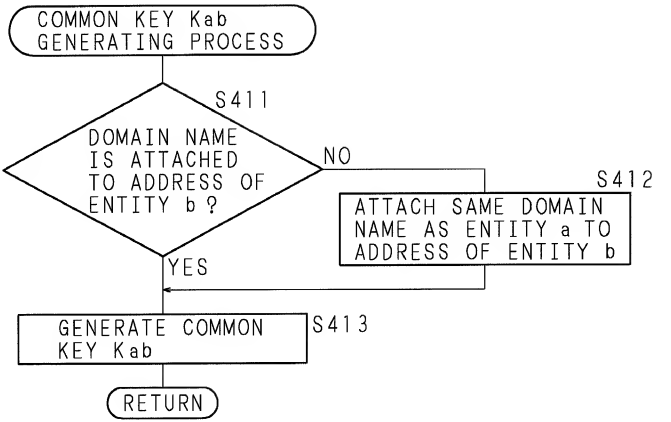
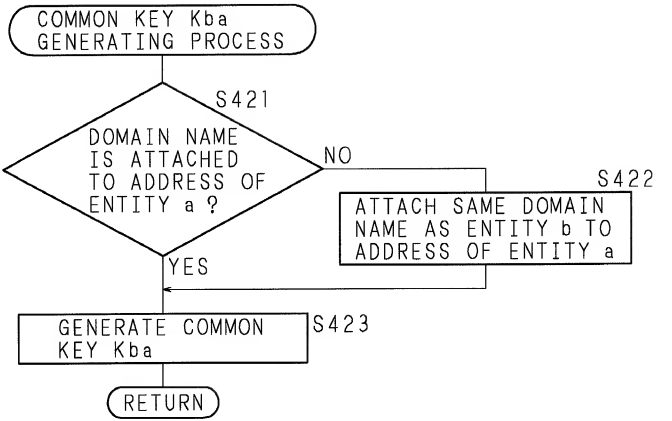

COMMON KEY Kab GENERATING PROCESS
S411
DOMAIN NAME IS ATTACHED TO ADDRESS OF ENTITY b ?
NO
S412
ATTACH SAME DOMAIN NAME AS ENTITY a TO ADDRESS OF ENTITY b
YES
GENERATE COMMON KEY Kab
S413
RETURN

FIG. 12


COMMON KEY Kba GENERATING PROCESS
S421
DOMAIN NAME IS ATTACHED TO ADDRESS OF ENTITY a ?
NO
S422
ATTACH SAME DOMAIN NAME AS ENTITY b TO ADDRESS OF ENTITY a
YES
GENERATE COMMON KEY Kba
S423
RETURN

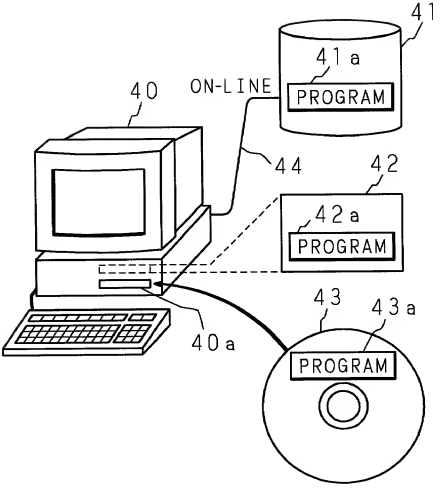



FIG. 13